GENERAL SERVICES ADMINISTRATION
Washington, DC 20405

CIO 2101.2
September 3, 2019

GSA ORDER

SUBJECT: GSA Enterprise Information Technology Management (ITM) Policy

1. Purpose.

a. In accordance with the Federal Information Technology Acquisition Reform Act (FITARA), Pub. L. No. 113-291, this Order outlines the authorities, responsibilities, and policies for management of all General Services Administration (GSA) Information Technology (IT) solutions, resources, and shared services.

b. IT will be managed in accordance with all statutory, regulatory, Office of Management and Budget (OMB), and agency requirements, including but not limited to FITARA. This Information Technology Management (ITM) Policy, along with associated processes, will be administered by the GSA Chief Information Officer (CIO) with support from applicable Services and Staff Offices (SSOs).

2. Cancellation. This Order cancels and supersedes CIO 2101.1, GSA Enterprise Information Technology Management (ITM) Policy, dated July 14, 2017; CIO 2102.1, Information Technology (IT) Integration Policy, dated March 9, 2015; and CIO-IL-16-02, Information Technology Shared Services Agreements, dated September 7, 2018.

3. Revisions. The following changes have been made to the Order.

a. Applicability and scope have been clarified.

b. Responsibilities have been revised to add governance, interagency-agreements (IAAs), and contract approval responsibilities for the CIO.

c. References have been updated.

d. Appendix A has been updated and renamed to add specific CIO roles.

e. Appendices B and C have been added to provide IT-specific definitions and policy guidance for submitting IT shared services agreements to the CIO for review.

4. Background.

a. In accordance with FITARA, the CIO is required to perform a significant role in agency IT decisions: including annual and multi-year planning, programming, budgeting, execution, reporting, management, governance, and oversight functions. (See Appendix A for detailed responsibilities from FITARA and other authorities).

b. To establish consistent agency interpretation for the scope of the covered areas, this policy uses the definitions of "information technology" and other terms from OMB M-15-14, Management and Oversight of Federal Information Technology. (See Appendix B for IT definitions).

5. Applicability.

a. This policy applies to:

(1) All GSA SSOs, including Regional Offices, and all GSA Federal employees and contractors;

(2) The Office of Inspector General (OIG) to the extent that the OIG determines it is consistent with the OIG's independent authority under the IG Act, and it does not conflict with other OIG policies or the OIG mission; and

(3) The Civilian Board of Contract Appeals (CBCA) to the extent that the CBCA determines it is consistent with the CBCA's independent authority under the Contract Disputes Act, and it does not conflict with other CBCA policies or the CBCA mission.

b. This policy applies to all IT resources, solutions, and/or services, and all activities pertaining to IT acquisition planning; IT budget formulation and execution; IT personnel resourcing and workforce development; IT development and enhancement activities; and operation and disposal of IT resources of any size where GSA is responsible for managing, hosting, and/or funding the work. (See Appendix B for definitions and examples of "IT resources, solutions, and/or services").

6. Responsibilities.

a. The CIO is responsible for:

(1) Promulgating policy addressing IT leadership and accountability, IT strategic planning, IT workforce, IT budgeting, investment management, and information security;

(2) Designating GSA IT officials to serve as liaisons between the GSA lines of business and GSA IT in order to facilitate interactions such as reviewing incoming requests, advising on IT strategies, conducting IT portfolio or budget reviews, conducting project/program reviews, and other IT functions;

(3) Overseeing and managing internal delivery and performance management of IT initiatives, to include but not limited to, IT commodities, IT services, internet or

network-based solutions, telecommunications, and business or core mission systems;

(4) Participating in governance and management processes to review and concur on IT strategies and budgets managed across GSA; and

(5) Reviewing and approving contracts or other agreements for IT resources, IT services, or spending by GSA SSOs, in conjunction with applicable procurement groups, the Chief Acquisition Officer (CAO) and the Chief Financial Officer (CFO). (See Appendix C for further information on IT shared services agreements).

b. CIO approval must be obtained before entering into any contracts or other agreements for all major IT investments. This approval **cannot** be delegated. Approval for non-major IT investments, as defined in OMB's annual IT capital planning guidance, may be delegated to the Deputy CIO (See ADM 5450.39D, GSA Delegations of Authority Manual). Non-major IT investments are those that do not require special management attention because of their importance to the mission or function to the Government; high executive visibility; high development, operating or maintenance costs; or unusual funding mechanisms (OMB M-15-14). GSA's Capital Planning and Investment Control (CPIC) guide has additional GSA-specific guidance.

c. All SSOs are responsible for:

(1) Ensuring appropriate business planning and management of business requirements to guarantee transparency, accountability, and coordination with the CIO, and/or appointed delegate(s), throughout the IT lifecycle;

(2) Collaborating with the CIO, and/or appointed delegate(s), regarding organizational plans or changes that have an impact on the delivery of IT systems or solutions for IT initiatives that are managed outside of GSA IT; and

(3) Implementing standardized processes to ensure that:

(a) Before entering into any contract or other agreement for IT or IT services, the contract or agreement has undergone the required CIO review and obtained the required approval. (See ADM 5450.39D, GSA Delegations of Authority Manual).

(b) Before requesting the allocation or reprogramming of any funds made available for IT programs, systems, solutions, resources, and/or shared services, the request has undergone the required CIO review and obtained the required approval. (See ADM 5450.39D, GSA Delegations of Authority Manual).

7. Policy. This policy ensures compliance with FITARA and other regulations for all planned or existing IT systems, solutions, resources, and shared services, regardless of budget source, size, complexity or significance, in all of its acquisitions or solutions life-cycle phases.

8. References.

a. Federal Information Technology Acquisition Reform Act (FITARA), Pub. L. 113-291

b. Clinger-Cohen Act of 1996, (formerly called the Information Technology Management Reform Act of 1996), codified at 40 U.S.C. § 11101, *et seq*

c. Federal Information Security Modernization Act (FISMA) of 2014, Pub. L. 113-283

d. GAO-04-394G, Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity

e. GAO-18-93, Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities

f. OMB Circular A-11, Preparation, Submission, and Execution of the Budget

g. OMB Circular A-123, Management's Responsibility for Internal Control

h. OMB Circular A-130, Managing Information as a Strategic Resource

i. OMB M-19-03, Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program

j. OMB M-19-16, Centralized Mission Support Capabilities for the Federal Government

k. OMB M-19-18, Federal Data Strategy - A Framework for Consistency

l. OMB M-15-14, Management and Oversight of Federal Information Technology

m. ADM 5450.39D, GSA Delegations of Authority Manual

n. Executive Order 13833, Enhancing Effectiveness of Agency Chief Information Officers

o. Executive Order 13873, Securing the Information and Communications Technology and Services Supply Chain

9. Signature.

/S/_____
DAVID SHIVE
Chief Information Officer
Office of GSA IT

Appendix A - CIO Responsibilities

1. The CIO and GSA IT's responsibilities under FITARA, OMB M-15-14, and other authorities include:

   a. IT Leadership and Accountability. (See FITARA, Clinger-Cohen Act of 1996, OMB M-15-14, A-130)

      (1) Report directly to the agency head or that official's deputy, if authorized.

      (2) Assume responsibility and accountability for IT investments.

      (3) In conjunction with the CFO, define the level of detail with which IT resource levels are described distinctly from other resources throughout the planning, programming, and budgeting stages.

      (4) Designate a senior agency information security officer.

   b. IT Strategic Planning. (See FITARA, OMB M-15-14, A-130)

      (1) Establish goals to improve agency operations through IT.

      (2) Measure how well IT supports agency programs.

      (3) Prepare an annual report on the progress in achieving the goals.

      (4) Benchmark agency processes against private and public sector performance.

      (5) Ensure that agency processes are analyzed and revised as appropriate before making significant IT investments.

   c. IT Workforce. (See OMB M-15-14, A-130)

      (1) Annually assess the extent to which agency personnel meet IT management knowledge and skill requirements.

      (2) Annually develop strategies for hiring and training to rectify any knowledge and skill deficiencies.

      (3) Annually report to the head of the agency on progress made in improving IT personnel capabilities.

   d. IT Budgeting. (See FITARA, OMB M-15-14, A-130)

      (1) Have a significant role in IT planning, programming, and budgeting decisions.

(2) Ensure that the agency implements a process for selecting IT investments.

(3) Review and approve the IT budget request.

(4) Review and approve funding reprogramming requests.

e. IT Investment Management. (See FITARA, OMB M-15-14, A-130)

(1) Have a significant role in IT execution decisions and the management, governance, and oversight processes related to IT.

(2) Improve the management of the agency's IT through portfolio review (PortfolioStat).

(3) Implement a process for controlling and evaluating IT investments.

(4) Evaluate IT investments to ensure projects are effectively managed (IT Dashboard CIO Ratings).

(5) Review high-risk IT investments.

(6) Certify that IT investments are adequately implementing incremental development, as defined in capital planning guidance issued by OMB.

(7) Advise head of the agency on whether to continue, modify, or terminate any acquisition, investment, or activity that includes a significant IT component based on the CIO's evaluation.

(8) Coordinate with the agency head and CFO to ensure that the financial systems are effectively implemented.

(9) Review and approve contracts or other agreements for IT or IT services, acquisition strategies, and acquisition plans.

(10) Maintain an inventory of data centers and strategy to consolidate and optimize data centers.

f. Information Security. (FISMA of 2014)

(1) Develop and maintain an agency-wide information security program.

(2) Develop and maintain information security policies, procedures, and control techniques.

(3) Ensure that senior agency officials, including ACIOs, Authorizing Officials (AOs) or equivalent officials, carry out their information security responsibilities.

(4) Ensure that agency personnel, including those with significant responsibility for information security, are trained to effectively carry out information security policies, procedures, and control techniques.

(5) Ensure that all personnel are held accountable for complying with the agency-wide information security program.

(6) Report annually to the agency head on the effectiveness of the agency information security program.

Appendix B - Information Technology (IT) Definitions

1. For the purposes of this policy, “information technology” is based on the definition of information technology found in OMB M-15-14 and the Clinger-Cohen Act of 1996, and refers to:

a. Any services or equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency where services or equipment are used by the agency directly or by a contractor with the agency that requires use of the services or equipment to a significant extent in the performance of a service or the furnishing of a product.

b. Computers and ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance); peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including provisioned services such as cloud computing and support services that support any point of the lifecycle of the equipment or service); and related resources.

c. Building Automation System (BAS) IT, including: Computer hardware and computer software that support BAS; BAS components, sensors and devices that are assigned an IP address and reside on the GSA network; Network wiring and other networking components that connect BAS devices to the GSA network; and service contracts that install, maintain and remove BAS hardware, software or components.

d. The term “information technology” does not include any equipment that is acquired by a contractor incidental to a contract that does not require use of the equipment.

2. To establish a consistent government-wide interpretation of the Federal resources included in this scope, the following OMB M-15-14 definition, based on the Clinger-Cohen Act of 1996, shall be used to define “information technology resources, solutions, and/or services” to include all:

a. Agency budgetary resources, personnel, equipment, facilities, or services that are primarily used in the management, operation, acquisition, disposition, and transformation, or other activity related to the lifecycle of information technology;

b. Acquisitions or IAAs that include information technology and the services or equipment provided by such acquisitions or IAAs; except assisted IT acquisition services IAAs where GSA is not responsible for managing, hosting, or funding the work;

c. Does not include grants to third parties which establish or support information technology not operated directly by the Federal Government;

d. Does not include skills or functions as part of the GSA program or business lines such as: requiring ancillary knowledge of IT systems, concepts and/or methods to carry out program or business line mission requirements; providing business analytical support such as requirements definition and analysis, necessary to ensure technology supports business needs; providing expertise on business/program specific applications as advanced users or program experts versus technical IT staff; and inputting data content (e.g., content for web pages, business/program specific data, etc.).

Appendix C - Shared Services Agreements

1. This policy applies to IT shared services agreements, which are agreements entered into between GSA and other Federal agencies in which GSA agrees to provide IT services to another Federal agency on a reimbursable basis, through Interagency Agreements (IAAs), Memoranda of Understanding (MOU) or Agreement (MOA). This policy does not apply to assisted acquisitions conducted by GSA on behalf of another Federal agency or to other agency purchases directly from a GSA acquisition vehicle. All proposed shared services agreements will be documented in an Interagency Agreement (IAA), Memorandum of Understanding (MOU), or Memorandum of Agreement (MOA).

a. Shared services agreements shall document reimbursable agreements between two Federal agencies. The agreement establishes the general terms and conditions that manage the relationship between the two agencies, justifies the need, and authorizes the transfer and obligation of funds.

b. According to the Department of Treasury Interagency Agreement Guide:

(1) Interagency Agreement (IAA): A written agreement entered into between two Federal agencies, or major organizational units within an agency, which specifies the goods to be furnished or tasks to be accomplished by one agency (the servicing agency) in support of the other (the requesting agency) The Bureau of the Fiscal Service within the Treasury Department provides step-by-step instructions on how to use IAA forms.

(a) Form 7600A. This form serves as an umbrella agreement. It includes provisions and information that will apply for all orders placed under the umbrella agreement. It does not replace an order and does not obligate funds. Offices may place multiple orders placed under one umbrella 7600A, or only a one-time order.

(b) Form 7600B. This is the order and funding obligation document for specific goods or services. The requesting agency's funds are obligated when the order is placed. Each order requires a separate 7600B. If the Requesting Agency or Office intends to obligate funds whose availability expires at the end of the current fiscal year on an IAA, an umbrella 7600A will require annual orders.

(2) MOA / MOU. MOAs/MOUs are agreements between agencies or bureaus that do not involve payment or transfer of funding. If the agreement involves funding, an IAA shall be executed.

2. All proposed shared services agreements for IT or IT services shall be reviewed and approved/concurred with by the applicable Head of Service and Staff Office before being submitted to the CIO for review and approval. Review and concurrence by the Office of General Counsel is strongly encouraged.

3. If the IT shared services agreement does not utilize GSA's environment, then the appropriate GSA stakeholders should ensure the partner agency has reviewed and approved the agreement in accordance with FITARA.

4. When a GSA business line endorses the shared services being proposed, in addition to the IAA, there should be sufficient internal funds and resources documented to support the work.

5. All shared services agreements for major IT investments will require CIO review and approval. Review and approval of non-major IT investments may be delegated to the DCIO. In addition, certain OMB-recognized IT shared services agreements, such as the Human Resources Line of Business shared services agreement, will require approval from OMB (See OMB M-19-16). In this case, following the appropriate internal reviews, GSA IT will forward the formally recognized IT shared services agreement to OMB for approval.

6. GSA IT Leadership will annually review the inventory of IT agreements for compliance with FITARA guidance.